

What is claimed is:

1 1. A content decryption device that decrypts encrypted
2 content that is recorded on a recording medium, and outputs the
3 decrypted content to an external device, comprising:

4 decryption means for decrypting the encrypted content to
5 generate the decrypted content; and

6 instruction execution means for decoding a transfer
7 instruction that includes a transfer destination address
8 showing a position of a content output means in an address space
9 as a transfer destination of the decrypted content to extract
10 the transfer destination address, and outputting the extracted
11 transfer destination address to an address detection means;

12 the address detection means for pre-storing a permitted
13 address that shows a transfer destination to which output of
14 the decrypted content is permitted, judging whether the
15 transfer destination address matches the permitted address, and
16 outputting, only when the transfer destination address matches
17 the permitted address, the decrypted content to the content
18 output means whose position is shown by the transfer destination
19 address; and

20 the content output means for receiving the decrypted
21 content, and outputting the received decrypted content to the
22 external device.

1 2. The decryption device of Claim 1 further comprising:
2 obtaining means for obtaining, from another external
3 device, a decryption program including (a) a decryption
4 instruction that shows decryption of encrypted content, and (b)
5 a transfer instruction that includes the transfer destination
6 address showing the position in the content output means, and
7 that shows transfer of the decrypted content to the content
8 output means,
9 wherein the decryption means decrypts the encrypted
10 content according to the decryption instruction, and
11 the instruction execution means outputs the transfer
12 destination address according to the transfer instruction.

1 3. The content decryption device of Claim 2,
2 wherein the decryption means, the instruction execution
3 means, the address detection means, the content output means
4 and the obtaining means are connected via a bus,
5 the instruction execution means outputs the transfer
6 destination address via the bus,
7 the address detection means obtains the transfer
8 destination address via the bus, and outputs the decrypted
9 content via the bus, and
10 the content output means receives the decrypted content

11 via the bus.

1 4. The content decryption device of Claim 3,
2 wherein the address detection means further has a state
3 in which the permitted address is not stored, and
4 the content decryption device further comprises:
5 state control means for judging whether the address
6 detection means stores the permitted address, and, when the
7 address detection means is judged not to store the permitted
8 address, prohibiting the instruction execution means from
9 executing the transfer instruction.

1 5. The content decryption device of Claim 3,
2 wherein the obtaining means further obtains, from the
3 other external device, an encrypted permitted address that is
4 a new permitted address which has been encrypted,
5 the decryption means decrypts the encrypted permitted
6 address to generate the new permitted address,
7 the address detection means stores the generated new
8 permitted address in place of the permitted address, and when
9 encrypted content is next decrypted, judges whether the
10 transfer destination address and the new permitted address
11 match.

1 6. The content decryption device of Claim 5,
2 wherein the decryption means pre-stores a variable key,
3 and decrypts the encrypted permitted address using the variable
4 key.

1 7. The content decryption device of Claim 6,
2 wherein the decryption means further pre-stores a unique
3 key that is unique to the content decryption device,
4 the obtaining means further obtains an encrypted variable
5 key that is a new variable key that has been encrypted using
6 the unique key,
7 the decryption means decrypts the encrypted variable key
8 using the unique key to generate the new variable key, and stores
9 the generated new variable key in place of the variable key,
10 and uses the new variable key when next decrypting a permitted
11 address that has been encrypted using the new variable key.

1 8. The content decryption device of Claim 6,
2 wherein the decryption means further has a state in which
3 the variable key is not stored, and
4 the state control means further judges whether the
5 decryption means stores the variable key, and, when the
6 decryption means is judged not to store the variable key,
7 prohibits the decryption means from decrypting.

1 9. The content decryption device of Claim 1,
2 wherein the decryption means, the instruction execution
3 means and the address detection means together compose a CPU,
4 a first authentication is performed between the CPU and
5 the recording medium, and following the first authentication
6 a second authentication is performed between the CPU and the
7 content output unit, and

8 the content decryption device decrypts the encrypted
9 content and outputs the decrypted content to the external device
10 only when both the first authentication and the second
11 authentication are successful.

1 10. A content decryption device that decrypts encrypted
2 content and outputs the decrypted content to an external device,
3 comprising:

4 obtaining means for obtaining, from another external
5 device, a decryption program that includes a program for
6 decrypting encrypted content and outputting the decrypted
7 content to the external device, and that includes first
8 encrypted information and second encrypted information, the
9 first encrypted information having been generated by encrypting
10 a predetermined piece of information according to a first
11 encryption, the second encrypted information having been

12 generated by encrypting the predetermined piece of information
13 according to a second encryption;
14 storage means for storing the program;
15 decryption means for decrypting the first encrypted
16 information according to a first decryption to generate first
17 decrypted information, and decrypting the second encrypted
18 information according to a second decryption to generate second
19 decrypted information, the first decryption being an inverse
20 transformation of the first encryption, and the second
21 decryption being an inverse transformation of the second
22 encryption; and
23 judgement means for judging whether the first decrypted
24 information and the second decrypted information match, and
25 when the first decrypted information and the second decrypted
26 information are judged not to match, prohibiting execution of
27 the program.

1 11. The content decryption device of Claim 10,
2 wherein the first encryption is encryption in which a
3 predetermined encryption algorithm is applied using a first
4 key,
5 the second encryption is encryption in which the
6 predetermined encryption algorithm is applied using a second
7 key,

8 the first decryption is decryption in which a
9 predetermined decryption algorithm is applied using a first key,
10 the predetermined decryption algorithm being an inverse
11 transformation of the predetermined encryption algorithm, and
12 the second decryption is decryption in which the
13 predetermined decryption algorithm is applied using a second
14 key.

12. The content decryption device of Claim 10,
wherein the first encryption is encryption in which a
first encryption algorithm is applied using an encryption key,
the second encryption is encryption in which a second
encryption algorithm is performed using the encryption key,
the first decryption is decryption in which a first
decryption algorithm is performed using the encryption key, the
first decryption algorithm being an inverse conversion of the
first encryption algorithm, and
the second decryption is decryption in which the second
decryption algorithm is performed using the encryption key, the
second decryption algorithm being an inverse conversion of the
second encryption algorithm.

1 13. The content decryption device of Claim 10, further
2 comprising:

3 control means for executing initialization of the content
4 decryption device when the judgement means judges that the first
5 decrypted information and the second decrypted information do
6 not match.

1 14. The content decryption device of Claim 10,
2 wherein the control means further, when the first
3 decrypted information and the second decrypted information are
4 judged not to match, requests the user to have the program stored
5 in the storage means.

1 15. The content decryption device of Claim 14,
2 wherein the control means further judges whether the
3 program has been updated, and, when the program is judged not
4 to have been updated, prohibits execution of the program.

1 16. A content decryption device that decrypts encrypted
2 content and outputs the decrypted content to an external device,
3 comprising:
4 data storage unit for storing (a) a first encrypted key
5 that has been generated by encrypting a common key using a CPU
6 unique key that is unique to a CPU, and (b) a second encrypted
7 key that has been generated by encrypting a common key using
8 a content processing unit unique key that is unique to a content

9 processing unit;
10 the CPU for performing execution of instructions,
11 encryption of information, and decryption of information, and
12 for generating a common key by decrypting the first encrypted
13 key using the CPU unique key, and storing the generated common
14 key,
15 the content processing unit for (a) storing content, or
16 outputting stored content to the external device, and (b)
17 generating a common key by decrypting the second encrypted key
18 using the content processing unit unique key.

1 17. The content decryption device of Claim 16,
2 wherein the CPU includes:
3 a key generation sub-unit for generating a new common key;
4 an encryption sub-unit for encrypting the new common key
5 using the common key to generate an encrypted common key;
6 an output sub-unit for outputting the generated encrypted
7 common key to the content processing unit; and
8 a key updating sub-unit for storing the new common key
9 in place of the common key; and
10 the content processing unit includes:
11 an obtaining sub-unit for obtaining an encrypted common
12 key;
13 a decryption sub-unit for decrypting the obtained

14 encrypted common key using the common key to generate a new
15 common key; and

16 a key updating sub-unit for storing the new common key
17 in place of the common key.

1 18. The content decryption device of Claim 16,
2 wherein the CPU includes:

3 an information storage sub-unit for storing
4 predetermined information;

5 an encryption unit for encrypting the predetermined
6 information using the common key to generate encrypted
7 information;

8 an output sub-unit for outputting the generated encrypted
9 information to the content processing unit; and

10 a key calculation sub-unit for applying a predetermined
11 calculation to the common key and the predetermined information
12 to generate a new common key, and storing the generated new
13 common key in place of the common key, and

14 the content processing unit further includes:

15 an obtaining sub-unit for obtaining encrypted
16 information;

17 a decryption sub-unit for decrypting the obtained
18 encrypted information using the common key to generate a new
19 common key; and

20 a key calculation sub-unit for applying a predetermined
21 calculation that is the same as the predetermined calculation
22 to the common key and the predetermined information to generate
23 a new common key, and storing the generated new common key in
24 place of the common key.

CONFIDENTIAL